The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
08/04/2016

SUBJECT:
Multiple Vulnerabilities in Mozilla Firefox Could Allow for Arbitrary Code Execution

OVERVIEW:
Multiple vulnerabilities have been identified in Mozilla Firefox and Firefox ESR, which could allow for arbitrary code execution. Mozilla Firefox is a web browser used to access the Internet. Mozilla Firefox ESR is a version of the web browser intended to be deployed in large organizations. Exploitation of these vulnerabilities could allow an attacker to bypass same-origin policy restrictions to access data, and execute arbitrary code in the context of the affected application.

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEM AFFECTED:

- Mozilla Firefox versions prior to 48
- Mozilla Firefox ESR versions prior to 45.3

RISK:
Government:

- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:
Mozilla has confirmed multiple vulnerabilities in Firefox and Firefox ESR. Exploitation of these vulnerabilities could allow for arbitrary code execution, bypass the same-origin policy and other security restrictions, and perform unauthorized actions. These vulnerabilities could be exploited if a user visits or is redirected to a specially-crafted webpage or opens a specially-crafted file. Details of these vulnerabilities are as follows:

- A same-origin security-bypass vulnerability that occurs when a local HTML file resides in the same directory as a malicious local shortcut file, and the local page calls the shortcut. An attacker can this issue to read the contents of local files or directories or to load an arbitrary website. (CVE-2016-5265)
- A security-bypass vulnerability that occurs when JaveScript event handler attributes on <marquee> tag execute inside a sandboxed iframe that does not have the allow-scripts flag set. (CVE-2016-5262)
- A buffer-overflow vulnerability in the ClearKey Content Decryption Module (CDM) used by the Encrypted Media Extensions (EME) API. An attacker can exploit this vulnerability when combined with a second vulnerability that allows an escape from the Gecko Media Plugin Sandbox. Combining the two can allow for arbitrary code execution. (CVE-2016-2837)
- A denial-of-service vulnerability that occurs due to a type confusion flaw in display transformation during rendering, due to incorrect bounds checking. (CVE-2016-5263)
- A denial-of-service vulnerability due to an use-after-free error when applying effects to SVG elements. (CVE-2016-5264)
- A denial-of-service vulnerability due to an use-after-free error when working with nested sync event loops in Service Workers. (CVE-2016-5259)
- A denial-of-service vulnerability due to an use-after-free error during WebRTC session shutdown when DTLS objects in memory are freed. (CVE-2016-5258)
- A use-after-free memory-corruption vulnerability when the 'alt' key is used in conjunction with toplevel menu items in Firefox. (CVE-2016-5254)
- A stack-based buffer-underflow vulnerability that occurs when calculating clipping regions in 2D graphics. (CVE-2016-5252)
- A memory-corruption vulnerability because of improper decoding using the LibAV library included in version 0.10 of the FFmpeg library on Linux systems. (CVE-2016-2839)
- Multiple memory-corruption vulnerabilities which occur due to memory safety bugs. (CVE-2016-2836, CVE-2016-2835)
- An information disclosure vulnerability occurs due to retained network connection. Specifically, the issue occurs in 'Favicon network connection'. (CVE-2016-2830)
- A buffer-overflow vulnerability exists when rendering SVG format graphics with directional content. (CVE-2016-2838)
- An information-disclosure vulnerability that occurs because the URLs of resources loaded after a navigation started (such as in an unload event handler) were leaked to the following page through the Resource Timing API. (CVE-2016-5250)
- A spoofing vulnerability that affects some of the special about: URLs used by Firefox to display system information or error messages can incorporate text passed as parameters. (CVE-2016-5268)
- An address bar spoofing vulnerability that occurs in Firefox for Android when using right-to-left character sets when combined with left-to-right characters. This can be used to cause only certain portions of the loaded left-to-right character portion of the URL to be displayed, misleading users as to what site is loaded, possibly leading to phishing attacks. (CVE-2016-5267)
- An information-disclosure vulnerability that occurs when the file URIs dragged from a web page to other software do not have their contents properly filtered before being passed to other programs, such as the local file manager... (CVE-2016-5266)
- An integer-overflow vulnerability in WebSockets during data buffering on incoming packets. (CVE-2016-5261)
- An information-disclosure vulnerability when the session restore data stores the passwords in plain text. This issue occurs when a password input field on a page has its type changed from 'password' to 'text' during a session. (CVE-2016-5260)

- A local arbitrary file-overwrite vulnerability when the Updater is opened directly using the callback application path parameter, a copy of a user specified file is made as a callback file. If the target of this file is made with a locked hardlink, an arbitrary local file can be replaced on the system even if there is no privileged write access to the targeted file. If this targeted file is run by other processes with privileges, this could allow for arbitrary code execution by a malicious user with local system access. (CVE-2016-5253)
- An information-disclosure vulnerability due to an out-of-bounds read error in Expat library. Specifically, this issue occurs when parsing malformed XML data during character conversion. (CVE-2016-0718)
- A location bar spoofing vulnerability that occurs when decoding url-encoded values in data: urls for display leads to potential spoofing in the Location bar by using non-ASCII and emoji characters in a data: url's mediatype. This issue could result in the wrong URL being displayed as a location, which can mislead users to believe they are on a different site than the one loaded. (CVE-2016-5251)
- A use-after-free vulnerability caused by how objects and pointers are handled in JavaScript during incremental garbage collection in some circumstances working with object groups. (CVE-2016-5255)

Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Customers whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate updates provided by Mozilla to vulnerable systems, immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.

REFERENCES:

Mozilla:
https://www.mozilla.org/en-US/security/advisories/mfsa2016-62/
https://www.mozilla.org/en-US/security/advisories/mfsa2016-63/
https://www.mozilla.org/en-US/security/advisories/mfsa2016-64/
https://www.mozilla.org/en-US/security/advisories/mfsa2016-65/
https://www.mozilla.org/en-US/security/advisories/mfsa2016-66/
https://www.mozilla.org/en-US/security/advisories/mfsa2016-67/
https://www.mozilla.org/en-US/security/advisories/mfsa2016-68/
https://www.mozilla.org/en-US/security/advisories/mfsa2016-69/
https://www.mozilla.org/en-US/security/advisories/mfsa2016-70/
https://www.mozilla.org/en-US/security/advisories/mfsa2016-71/

https://www.mozilla.org/en-US/security/advisories/mfsa2016-72/
https://www.mozilla.org/en-US/security/advisories/mfsa2016-73/
https://www.mozilla.org/en-US/security/advisories/mfsa2016-74/
https://www.mozilla.org/en-US/security/advisories/mfsa2016-75/
https://www.mozilla.org/en-US/security/advisories/mfsa2016-76/
https://www.mozilla.org/en-US/security/advisories/mfsa2016-77/
https://www.mozilla.org/en-US/security/advisories/mfsa2016-78/
https://www.mozilla.org/en-US/security/advisories/mfsa2016-79/
https://www.mozilla.org/en-US/security/advisories/mfsa2016-80/
https://www.mozilla.org/en-US/security/advisories/mfsa2016-81/
https://www.mozilla.org/en-US/security/advisories/mfsa2016-82/
https://www.mozilla.org/en-US/security/advisories/mfsa2016-83/
https://www.mozilla.org/en-US/security/advisories/mfsa2016-84/

CVE:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0718
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2830
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2835
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2836
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2837
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2838
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2839
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5250
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5251
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5252
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5253
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5254
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5255
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5258
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5259
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5260
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5261
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5262
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5263
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5264
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5265
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5266
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5267
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5268